Shufti

Guide

Stablecoin AML Compliance Guide

Why Stablecoins require a different regulatory approach and what it means for identity and financial crime compliance

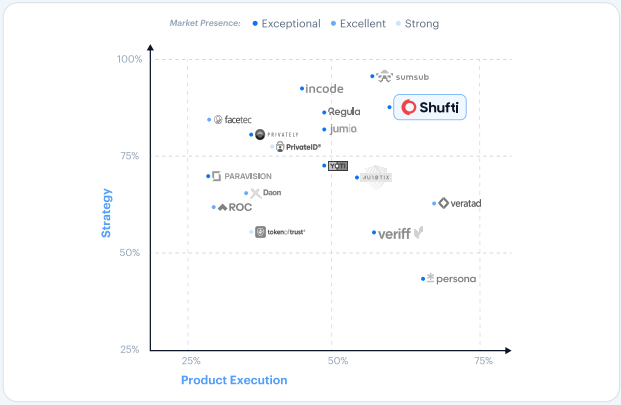


KJM AGE VERIFICATION | PCI DSS | iBeta L3 | ISO 27001:2022 | CE+ | QG GDPR | SOC2 | GDPR | CCPA

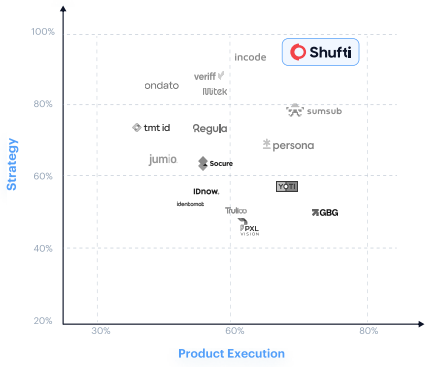
Industry Recognition 2025–2026

Recognised by leading analyst firms, government bodies and independent research organisations

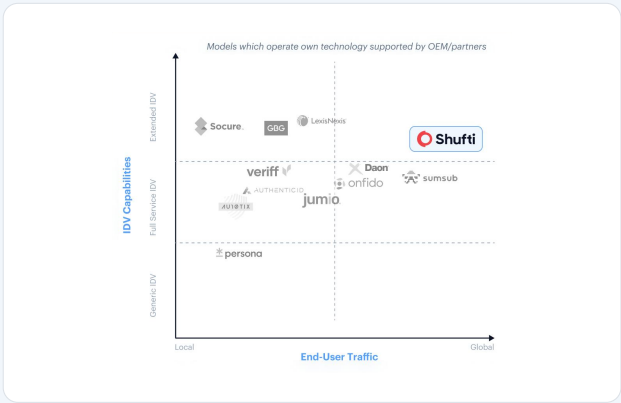
Ranked Exceptional in Liminal's 2026 Age Estimation Index



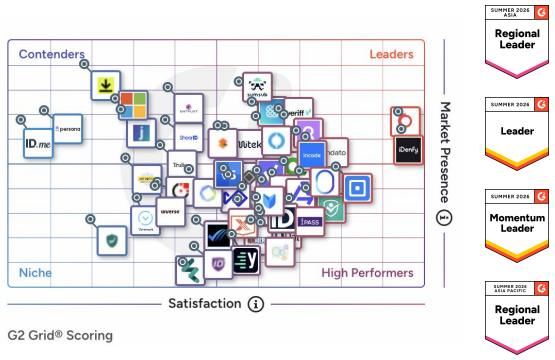
Ranked Exceptional in Liminal's 2026 Age Verification Index



Broadest global reach in the 2025 KuppingerCole Extended IDV report



Recognised as a Leader across four G2 Summer 2026 reports



Differentiated by Gartner on document diversity and country coverage



240+ Countries & Territories

10k+ Document Types

First EU company to achieve iBeta Level 3 Conformance to ISO/IEC 30107-3, with 0% APCER

iBeta Level 3 Conformance

0% APCER



Ranked Top 5 in the DHS RIVR 2025 for identity validation

0% Extraction Failure

0.67% Worst-Case FNMR



Copyright © Shufti. All Rights Reserved.

Table of Contents

01 Introduction to stablecoin regulation 03

02 Why Stablecoins Get Their Own Rule 06

03 The Main Type Of Stablecoins 07

04 How Major Markets Regulates Stablecoins 09

05 Stablecoin Regulatory Requirements By Sector 28

06 Unique AML/CFT Challenges For Businesses Operating In The Stablecoin Economy 43

07 Shufti As Compliance Infrastructure Across The Stablecoin Lifecycle 51

08 Stablecoin AML Compliance Solution Checklist 57

09 References 61

Disclaimer: This guide is for general information only and is not legal, regulatory or compliance advice. The rules it describes reflect their status in October 2026 and may change. Businesses should confirm their obligations with qualified advisers in each market they serve. Shufti's tools support compliance operations but do not by themselves ensure compliance with any law. Each regulated business remains responsible for meeting its own obligations.

Copyright © Shufti. All Rights Reserved.

1. Introduction to stablecoin regulation

For years, traditional finance and decentralised finance ran on separate tracks. Banks moved money through accounts and payment networks while crypto markets moved value on blockchains, so moving funds from one system to the other took several steps. Stablecoins are closing that gap because a fiat-backed stablecoin follows the value of a currency such as the US dollar and is backed by reserves held in the banking system. The token can therefore move on a blockchain at any hour while its holder can still swap it back into ordinary money. That combination has carried stablecoins well beyond crypto trading, into cross-border payments, remittances, business settlement, and trading and collateral in DeFi.

$ 317B

Stablecoin market capitalisation as of 6 April 2026, recorded in a Federal Reserve study.

$ 154B

Received by illicit crypto addresses in 2025, at a minimum.

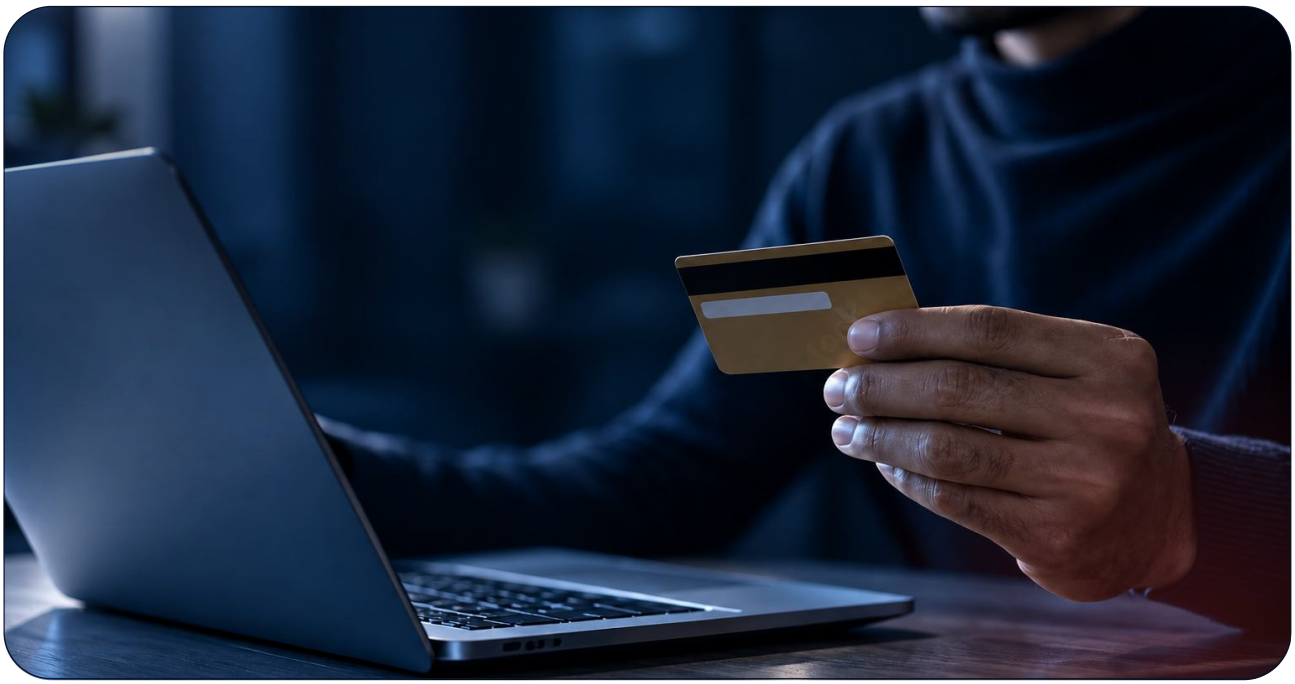
84%

Share of the illicit transaction volume identified that moved in stablecoins

A Federal Reserve study recorded a stablecoin market capitalisation of $317 billion as of 6 April 2026, which means a large pool of value now sits in tokens designed to behave like cash.

Copyright © Shufti. All Rights Reserved.

The same qualities that make stablecoins useful for payments are also drawing in illicit activity. Chainalysis's 2026 Crypto Crime Report found that illicit crypto addresses received at least $154 billion in 2025, and that stablecoins made up 84% of the illicit transaction volume it identified. The 84% figure measures how criminals choose to move funds once they are in crypto, so it shows where the risk is concentrating without indicating how much stablecoin use is criminal.



The Financial Action Task Force (FATF) notes that the stability, liquidity and ease of transfer that attract legitimate users also appeal to money launderers, terrorist financiers and sanctions evaders, particularly when funds hop between wallets and networks, pass through self-hosted wallets with no intermediary, or are cashed out through providers with weak controls. Under FATF standards, countries should bring businesses that exchange, hold or transfer stablecoins for customers under anti-money laundering rules, including the Travel Rule, which means sender and recipient details must travel with each transfer.

Copyright © Shufti. All Rights Reserved.

Regulators in major markets have now gone further and written rules specifically for stablecoins, although each market sits at a different stage of putting them into effect.

Country	Regulations	Status
European Union	Dedicated stablecoin rules already in force.	In Force
Hong Kong	Dedicated stablecoin rules already in force.	In Force
UAE	Regulates payment tokens through its central bank.	In Force
Brazil	Regulates the businesses that buy, sell and transfer stablecoins, and treats many stablecoin transactions as foreign exchange.	In Force
United States	Federal stablecoin law passed July 2025, expected to take effect by 18 January 2027.	Enacted
Canada	Federal stablecoin law passed March 2026, not yet in force.	Enacted
United Kingdom	New regime applies from 25 October 2027.	Upcoming
Singapore	Legislation to put its 2023 stablecoin framework into law is in progress.	Upcoming

This guide explains why regulators treat stablecoins differently, how each of these markets regulates them, and which identity and financial crime controls stablecoin issuers, banks, custodians and wallet providers, crypto exchanges, card issuers, payments and infrastructure platforms, and remittance providers need as a result.

Copyright © Shufti. All Rights Reserved.

2. Why stablecoins get their own rules

Crypto regulation already covers businesses that exchange, hold and transfer digital assets for their customers, but stablecoins raise a question those rules were never designed to answer: whether a token people use as money can keep its value and be swapped back for cash whenever the holder asks. When a stablecoin fails that test, the damage spreads well beyond crypto markets. Payments that depend on the token stall, and the stress travels through the reserves behind it, the banks that hold those reserves and the digital markets that rely on the token to settle.

Stablecoin-specific rules therefore concentrate on what backs the token, how those assets are safeguarded, how holders redeem and who governs the arrangement. Anti-money laundering, counter-terrorist financing and sanctions duties continue to come from the financial crime frameworks that already apply, supported by regulator guidance on how stablecoins move between customers, wallets, intermediaries and bank accounts. The two sets of obligations operate side by side, which means a business can sit entirely outside the reserve rules and still carry anti-money laundering duties for the stablecoin payments it handles.

Copyright © Shufti. All Rights Reserved.

3. The main types of stablecoins

Stablecoins hold their value in different ways, and what sits behind a token shapes its risks and, in many cases, how the law classifies it. Regulators therefore start by establishing which type of stablecoin they are assessing.

BACKED BY CASH AND DEPOSITS

Fiat-backed stablecoins

Tied to a currency and backed by reserves such as cash, bank deposits and approved short-term investments. This is the type most often used to move money between people and businesses, so it is the main focus of the payment and remittance examples in this guide.

BACKED BY DIGITAL ASSETS

Crypto-collateralised stablecoins

Backed by other digital assets, often worth more than the tokens issued, and rely on automatic sell-offs, known as liquidations, to protect that cushion. This structure carries quite different risks from a token backed by cash and redeemable for it.

BACKED BY GOLD OR A BASKET

Commodity- or asset-backed stablecoins

Track the value of gold or a basket of assets. Issuers set up these arrangements in different ways, so what the holder actually has a claim to, and how the law classifies the token, depends on the terms of each arrangement.

Copyright © Shufti. All Rights Reserved.

STABILISED BY CODE

Algorithmic and hybrid stablecoins

Use code that expands or shrinks the token supply to hold a target value, supported by incentives and, in some cases, a partial pool of collateral. The stablecoin label on its own says little about whether such a token qualifies under the regimes that regulate payment stablecoins.

Design labels like these describe how a token is built, while the law in each market draws its own lines. The EU, for example, separates tokens tied to a single currency from tokens tied to other assets or baskets, whereas other markets concentrate their rules on tokens tied to one currency. Tokenised bank deposits and central bank digital currencies are different products again, and regulators assess them separately.



Copyright © Shufti. All Rights Reserved.

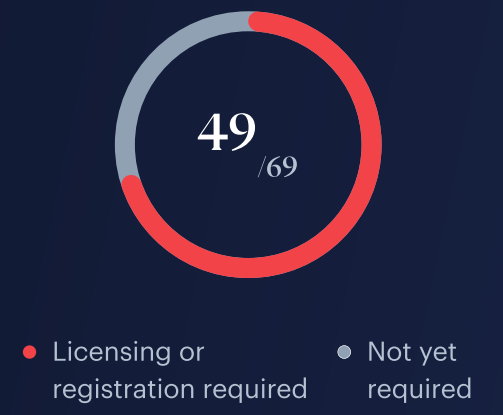
4. How major markets regulate stablecoins

Which rules apply depends on how the law classifies a token, what a business does with it and where it does that business. Only a relatively small number of jurisdictions have stablecoin-specific rules so far, while anti-money laundering and counter-terrorist financing (AML/CFT) coverage has moved faster. The FATF's July 2026 update tracks 69 jurisdictions, FATF members and others with materially important virtual asset activity, which together account for about 97% of the global market.

71%

In 71% of the jurisdictions the FATF tracks, stablecoin issuers must be licensed or registered when they qualify as virtual asset service providers.

49 OF 69 JURISDICTIONS [5]



Across the eight jurisdictions covered in this guide, stablecoin-specific rules and AML/CFT obligations may apply side by side, so a business serving customers in several countries will usually answer to several regimes at once. Each summary below reflects where things stand in October 2026.

> A stablecoin may fall under the oversight of both the authority responsible for virtual assets and a central bank or another financial regulator, with responsibilities divided differently in each jurisdiction according to the stablecoin's structure, its use in payments and its implications for financial stability.

Copyright © Shufti. All Rights Reserved.

FATF applies existing VASP standards to stablecoins and addresses their specific risks in a 2026 report

The FATF's Targeted Report on Stablecoins and Unhosted Wallets: Peer-to-Peer Transactions, published on 3 March 2026, applies the existing standards for virtual asset service providers (VASPs) to stablecoins and examines where stablecoins create distinct risks, from issuance and redemption to circulation through unhosted wallets.

FOCUS	WHAT THE REPORTS DICUSSES
Issuance and redemption	Preventive measures for customers buying or redeeming stablecoins directly with the issuer.
Secondary-market circulation	Risks arising after tokens move beyond the issuer's direct customers, particularly through unhosted wallets.
Issuer intervention	Technical capabilities to freeze, burn or withdraw stablecoins associated with illicit activity.
Smart-contract controls	Risk-based use of approved-address lists and blocked-address lists.
Responsibilities across the arrangement	The roles of issuers, intermediaries and other relevant participants.

The report also lists four warning signs, each of which a monitoring team can turn into specific alerts and then configure and test against its own customer activity.

Copyright © Shufti. All Rights Reserved.

FATF Warning Sign	Alert signals to configure
Fast cross-border movements that don't fit a customer's profile	▸ Funds received and sent on to another country within hours or days of arriving ▸ A corridor or destination country the customer has never used before ▸ Cross-border value well above the activity declared at onboarding
Unexplained switching between cash and stablecoins	▸ Repeated fiat to stablecoin to fiat round trips with no payment or treasury purpose ▸ A cash or fiat deposit converted to stablecoins and withdrawn to an external wallet almost straight away ▸ Conversions that start or stop abruptly with no change in the customer's stated business
Transfers between seemingly unrelated senders and recipients	▸ Many senders with no visible link paying the same recipient or wallet ▸ One sender paying many new recipients in a short period ▸ Recipients with no prior relationship, shared address or business link to the sender
Refunds sent to wallets unconnected to the original payer	▸ Refund address differs from the wallet that funded the original payment ▸ Refund wallet appears for the first time at the moment of the refund ▸ Refund requested shortly after payment, or repeated refunds on the same account

These alert signals are illustrative, so each team should calibrate and test them against actual customer activity.

Copyright © Shufti. All Rights Reserved.

AML/CFT REQUIREMENTS FOR STABLECOIN BUSINESSES

- Businesses must verify who their customers are before serving them and, for business customers, identify the beneficial owners, meaning the real people who ultimately own or control the company.

- Businesses must share and check Travel Rule details on every qualifying transfer. They also need a written plan for transfers that arrive with details missing, setting out when to hold such a transfer, when to ask for more information and when to reject it.

- Under the FATF's June 2025 update, which countries have until the end of 2030 to adopt, cross-border payments between individuals above USD or EUR 1,000 must carry the names, addresses and dates of birth of the people involved.

- Transfers to and from self-hosted wallets need extra care because customers control these wallets themselves, which leaves no provider on the other side to receive or confirm the customer's details.

Copyright © Shufti. All Rights Reserved.

The European Union regulates stablecoins and crypto service providers under MiCA

The EU's Markets in Crypto-Assets Regulation (MiCA) applies directly in every member state. Its stablecoin rules have applied since 30 June 2024 and its rules for crypto service providers since 30 December 2024. With the final grace period for firms operating under older national rules ending on 1 July 2026, MiCA is now fully in force.

STABLECOIN RULES

- MiCA recognises two types of stablecoin: e-money tokens, which are tied to a single official currency such as the euro, and asset-referenced tokens, which reference other values or rights, or combinations of them, such as a basket of currencies or commodities. Asset-referenced tokens are subject to specific reserve, capital and governance requirements.
- Only banks and licensed electronic money institutions may issue e-money tokens, and before offering a token they must publish a white paper, a disclosure document explaining how the token works. Issuers must issue tokens at face value when they receive funds and redeem them at face value whenever a holder asks, and they may not pay interest on the tokens.
- Issuers must hold at least 30% of the money they receive for e-money tokens as bank deposits, with the rest in safe, easy-to-sell investments. Very large tokens, which MiCA calls "significant", face extra rules and supervision by the European Banking Authority.
- Exchanges, custodians and transfer services generally need authorisation as a crypto-asset service provider (CASP), although certain already-regulated financial institutions can instead provide specified services through MiCA's notification procedure. Eligible providers can then operate across the EU once they complete the relevant cross-border notification requirements. Since 1 July 2026, regulators have expected firms without the required authorisation or regulatory permission to close their EU services in an orderly way. Firms outside the EU cannot serve EU customers except in very narrow cases, and the European Securities and Markets Authority (ESMA) keeps a public register of authorised providers.

Copyright © Shufti. All Rights Reserved.

AML/CFT REQUIREMENTS FOR STABLECOIN BUSINESSES

- E-money token issuers and CASPs must follow EU anti-money laundering law. Asset-referenced token issuers are not automatically covered solely because they issue ARTs, although their other activities or regulatory status may still bring them within scope. Businesses subject to these requirements must verify customers and their beneficial owners and assess each customer's risk. They must then apply extra checks to higher-risk customers and politically exposed persons (PEPs, meaning people in prominent public roles) and keep watching activity throughout the relationship. They must also report suspicious activity to their national Financial Intelligence Unit, keep records and follow applicable EU sanctions obligations.
- The Travel Rule applies to every crypto transfer between providers with no minimum amount, and EU rules name e-money tokens as covered.
- For transfers above EUR 1,000 to or from a self-hosted wallet, the provider must take adequate measures to assess whether its customer owns or controls that wallet.
- From 10 July 2027, the AMLR, a single EU anti-money laundering rulebook, will bring in harmonised AML/CFT requirements that apply directly. It bans anonymous crypto-asset accounts as well as accounts that anonymise their holders or hide transactions, including through anonymity-enhancing coins. From 2028, the Anti-Money Laundering Authority (AMLA) will directly supervise selected high-risk financial institutions and groups that operate across borders, potentially including CASPs.

Copyright © Shufti. All Rights Reserved.

The United Kingdom is building a two-part stablecoin regime

The UK's new crypto regime rests on regulations made in February 2026 and applies from 25 October 2027. The Financial Conduct Authority (FCA) published its final rules for the regime on 30 June 2026. The FCA will regulate qualifying stablecoin issuance from a UK establishment, while an issuer that HM Treasury recognises as systemic because of its importance to the financial system will be regulated jointly by the FCA and the Bank of England.

STABLECOIN RULES

- The rules cover issuers of "qualifying stablecoins", which are tied to a single currency, as well as the firms that hold the backing assets. Those assets must sit on statutory trust, which means the law ring-fences them for token holders, and firms must check them against the tokens in circulation every day. Issuers must complete the required AML/KYC checks and then place the redemption payment order by the end of the business day after the tokens reach the issuer's wallet. The deadline does not apply where meeting it would breach money laundering legislation.
- Firms already operating in the UK can apply for authorisation between 30 September 2026 and 28 February 2027 and keep operating while the FCA decides, provided they apply in this window. An existing anti-money laundering registration does not carry over automatically.
- The Bank of England's June 2026 policy sets a steady-state backing requirement for systemic stablecoins, under which at least 30% must sit in non-interest-bearing Bank deposits and up to 70% in short-term UK government debt. A phased approach lets eligible issuers recognised as systemic at launch hold a higher government-debt share at first. The policy also sets a temporary £40 billion issuance limit per systemic stablecoin, replacing the individual and business holding limits proposed in 2025. The Bank published the accompanying Code of Practice in draft and plans to finalise it by the end of 2026.

Copyright © Shufti. All Rights Reserved.

AML/CFT REQUIREMENTS FOR STABLECOIN BUSINESSES

- Many stablecoin businesses already need FCA registration under the UK's Money Laundering Regulations, well before the new regime starts. They include issuers that exchange their own tokens for money and firms that hold customers' tokens or private keys, the digital passwords that control a wallet. A payments licence alone does not cover these activities.
- Firms must assess money laundering risks across their business, verify customers and beneficial owners and keep monitoring activity over time, with extra checks for PEPs, customers linked to high-risk countries and other higher-risk situations.
- Under the UK Travel Rule, sender and recipient details must travel with crypto transfers, and the FCA has explained how firms should handle transfers that arrive with missing details.
- Firms must report suspicious activity, keep records and screen customers and transfers against UK sanctions lists, and the FCA expects to see these controls working when it reviews an application.

Copyright © Shufti. All Rights Reserved.

The United States regulates payment stablecoin issuers under the GENIUS Act

The GENIUS Act became law on 18 July 2025 and sets up a federal framework for payment stablecoins, under which only a permitted issuer may issue a payment stablecoin in the United States once the Act takes effect. Regulators are still writing the detailed rules, and Treasury expects the Act to take effect on 18 January 2027 unless final rules bring that date forward.

STABLECOIN RULES

- Issuers can qualify in three ways: as an approved subsidiary of an insured depository institution, including a bank or credit union; as a federally qualified issuer supervised by the Office of the Comptroller of the Currency (OCC); or as a state-qualified issuer. State issuers with up to $10 billion in circulation can operate under a state regime substantially similar to the federal framework. The Act also sets requirements for foreign issuers seeking US market access and for custodians holding reserves or private keys.
- Issuers must back every token at least one-to-one with eligible reserve assets, such as US dollars, bank deposits and short-term Treasury bills, and publish the make-up of their reserves monthly. They must also keep a published policy for timely redemption at the token's stated monetary value, and they may not pay interest or yield solely for holding, using or retaining the stablecoin.
- Issuers may not market a token as backed by the US government, protected by federal deposit insurance or legal tender.
- From 18 July 2028, digital asset service providers such as exchanges and custodians generally may only offer or sell payment stablecoins to US customers if the tokens come from permitted US issuers or foreign issuers meeting the Act's requirements.

Copyright © Shufti. All Rights Reserved.

AML/CFT REQUIREMENTS FOR STABLECOIN BUSINESSES

- Permitted payment stablecoin issuers will count as financial institutions under the Bank Secrecy Act, the main US anti-money laundering law, and will therefore need a compliance programme covering customer identification, due diligence, suspicious activity reporting and sanctions. They must also have the technical capabilities, policies and procedures to block, freeze and reject unlawful transactions.
- Treasury proposed detailed anti-money laundering and sanctions rules for issuers in April 2026 and customer identification rules in June 2026, and both remain at the proposal stage.
- Separately from the GENIUS Act, stablecoin businesses that qualify as money transmitters under existing US rules must already register with FinCEN and keep a written anti-money laundering programme with a designated compliance officer, staff training and independent testing.
- These money transmitters must also report suspicious activity and meet applicable Travel Rule requirements for passing on sender and recipient information. They must comply with OFAC sanctions through risk-based controls, such as appropriate screening of customers, counterparties and wallet addresses.

Copyright © Shufti. All Rights Reserved.

Singapore is turning its stablecoin framework into law

The Monetary Authority of Singapore (MAS) finalised its framework for qualifying single-currency stablecoins in August 2023. On 1 September 2026, it opened consultation on the legislation to implement the framework, which is not yet in force. Stablecoin rules

STABLECOIN RULES

- The framework covers stablecoins issued in Singapore and pegged to the Singapore dollar or a G10 currency, and qualifying tokens will be eligible for the "MAS-regulated stablecoin" label. Other stablecoins remain subject to the applicable digital-payment-token rules.
- The framework calls for full reserve backing, with requirements covering asset quality, custody, valuation and independent assurance, and issuers must also meet minimum capital and liquidity requirements.
- Issuers must return the tokens' face value within five business days of a redemption request and disclose their value-stabilisation arrangements, holders' rights and reserve-audit results.

Copyright © Shufti. All Rights Reserved.

AML/CFT REQUIREMENTS FOR STABLECOIN BUSINESSES

- MAS has stated that regulated stablecoin issuers will be subject to the existing AML/CFT standards that apply to digital-payment-token service providers and banks, including customer due diligence, screening and the Travel Rule.
- The September 2026 consultation adds a proposed stablecoin-specific requirement, under which issuers would need the technical capability to trace, freeze and/or burn issued tokens used for illicit activities, with a separate MAS notice setting out the detailed requirements.
- MAS is also seeking feedback on identifying every stablecoin holder, restricting unhosted wallets and monitoring tokens in circulation.
- Businesses already providing regulated digital-payment-token services involving stablecoins must meet the applicable existing AML/CFT requirements, including MAS Notice PSN02 where relevant, which cover customer checks, ongoing monitoring and suspicious-transaction reporting to Singapore's Suspicious Transaction Reporting Office.

Copyright © Shufti. All Rights Reserved.

Hong Kong licenses stablecoin issuers and limits who can offer them

Hong Kong's Stablecoins Ordinance took effect on 1 August 2025, and the HKMA granted the first two stablecoin issuer licences on 10 April 2026. Licensed issuers must meet both prudential requirements and a dedicated AML/CFT guideline covering stablecoin issuance, redemption and transfers.

STABLECOIN RULES

- Firms need a licence to issue fiat-referenced stablecoins in Hong Kong in the course of business, or Hong Kong dollar-referenced stablecoins outside Hong Kong. Only permitted providers may offer stablecoins, and only stablecoins from licensed issuers may be offered to retail customers.
- Reserve assets must fully back outstanding tokens and be segregated and protected through the required trust and custody arrangements. Issuers must publish reserve information weekly unless the HKMA agrees otherwise, obtain regular independent attestations and include reserves in their annual financial audit.
- Issuers must normally meet valid redemption requests at par within one business day, unless the HKMA permits otherwise, and they may not pay interest on their stablecoins.
- Non-bank issuers must meet the HK$25 million minimum capital requirement or the permitted equivalent financial-resource arrangement.

Copyright © Shufti. All Rights Reserved.

AML/CFT REQUIREMENTS FOR STABLECOIN BUSINESSES

- Licensed issuers must carry out customer due diligence before starting a business relationship, before occasional transactions of HK$8,000 or more, and where suspicion or doubts about identity information arise.
- Issuers' monitoring must cover issuance, redemption and stablecoins in circulation. Unless effective alternative controls satisfy the HKMA, each individual holder's identity must be verified by the issuer, an appropriately supervised financial institution or virtual-asset service provider, or a reliable third party.
- Issuers must assess customer wallets, verify ownership or control where required, screen unhosted wallet addresses and carry out due diligence on transfer counterparties.
- Stablecoin transfers must meet the applicable Travel Rule requirements, under which transfers below HK$8,000 need basic sender and recipient information and transfers at or above that threshold carry additional information and verification requirements.
- Issuers must maintain sanctions controls and report suspicious transactions to Hong Kong's Joint Financial Intelligence Unit.
- For issuance and redemption, funds and tokens must move through customers' pre-registered accounts and wallet addresses, and issuers must authenticate account operations and consider two-factor authentication proportionate to the risks.

Copyright © Shufti. All Rights Reserved.



The UAE divides stablecoin activity between several regulators

The Central Bank of the UAE (CBUAE) regulates payment-token services under rules effective from 31 August 2024. In Dubai, the Virtual Assets Regulatory Authority (VARA) regulates relevant virtual-asset activities outside the Dubai International Financial Centre (DIFC), while the DIFC and Abu Dhabi Global Market operate separate regimes. Dirham-referenced stablecoins fall under the CBUAE and sit outside VARA's issuance approval regime.

STABLECOIN RULES

- Under CBUAE rules, licensed dirham payment tokens may be used for lawful payments, whereas foreign payment tokens from registered issuers may be used as payment for virtual assets or their derivatives. The regulation also prohibits issuing algorithmic stablecoins and privacy tokens, or providing services involving them.
- Dirham-token reserves must fully cover outstanding tokens, and issuers must generally hold them as cash in a separate escrow account with an unrelated UAE bank. A wholly bank-owned issuer may instead hold at least 50% in cash and invest the rest in UAE government bonds and CBUAE M-bills with an average duration of six months or less.
- Issuers must redeem tokens at face value without delay and normally by the same time on the next business day, unless the CBUAE permits otherwise, and they may not pay interest on payment tokens.
- VARA's revised issuance rulebook took effect on 19 June 2025. Fiat-referenced virtual-asset issuers within its scope need the relevant licence and prior approval and must meet reserve, redemption and disclosure requirements.

Copyright © Shufti. All Rights Reserved.

AML/CFT REQUIREMENTS FOR STABLECOIN BUSINESSES

- CBUAE-regulated payment-token service providers must assess the risks linked to their tokens, services and customers, including anonymity, rapid cross-border transfers, peer-to-peer transactions and the use of multiple wallets.
- Providers must complete customer due diligence and may not start or continue a relationship where they cannot complete the required checks.
- Providers must screen transaction parties against applicable sanctions lists, meet freezing requirements and report suspicious activity to the UAE Financial Intelligence Unit.
- Compliance and money laundering reporting responsibilities must sit under senior-management oversight, and providers must assess risks before introducing new products or technologies. Digital onboarding is allowed where it meets CBUAE standards.
- VARA-licensed businesses carrying out relevant stablecoin activities must also comply with VARA's AML/CFT and Travel Rule requirements.

Copyright © Shufti. All Rights Reserved.

Canada has enacted a Stablecoin Act that is not yet in force

Canada's Stablecoin Act received Royal Assent on 26 March 2026 and sets up a future Bank of Canada registration and supervision regime. Its provisions are not yet in force, and commencement dates and implementation details will follow.

STABLECOIN RULES

- Once it takes effect, the Act will cover qualifying single-currency stablecoins with interprovincial or international applications, and in-scope issuers that are not financial institutions will need to register.
- Issuers will need full reserves in the reference currency or in qualifying liquid assets denominated in that currency, with custody and segregation protections.
- Issuers will have to redeem at par and provide monthly financial and reserve information, and they will not be allowed to pay holders interest or yield.

AML/CFT REQUIREMENTS FOR STABLECOIN BUSINESSES

- Section 5 will expressly bring in-scope issuers within Canada's AML framework as businesses dealing in virtual currencies.
- Registration applications will disclose previous AML/CFT enforcement actions, and the Bank of Canada will share completed applications with FINTRAC.
- Issuers will maintain policies that address money laundering and terrorist financing risks and provide those policies to the Bank of Canada.
- Existing businesses exchanging or transferring stablecoins must already meet applicable FINTRAC requirements where their activities fall within the virtual-currency regime, including customer verification, beneficial-ownership checks, ongoing monitoring, suspicious-transaction reporting and the Travel Rule.

Copyright © Shufti. All Rights Reserved.



Brazil regulates stablecoin intermediaries and treats many transfers as foreign exchange

Brazil primarily regulates the businesses that buy, sell, hold and transfer virtual assets, including stablecoins. BCB Resolutions 519, 520 and 521 introduced authorisation, operational and foreign-exchange requirements from 2 February 2026, with transitional arrangements for existing providers.

STABLECOIN RULES

- Virtual-asset service providers may operate as intermediaries, custodians or brokers combining those activities, and authorisation requirements apply to each model, although eligible existing businesses can continue under prescribed transition arrangements.
- Foreign-exchange rules cover specified activities, including buying, selling or exchanging fiat-referenced virtual assets, international crypto payments, settlement
  of card spending abroad and transfers involving self-hosted wallets. The related reporting requirements apply to operations from 3 November 2026, after the BCB moved the start date from 4 May 2026.
- International virtual-asset payments and transfers through SPSAVs are limited to US$100,000 equivalent where the counterparty is not authorised to operate in the foreign-exchange market.
- The resolutions do not create a standalone licensing and local-reserve regime for foreign stablecoin issuers, although an issuer's Brazilian activities may trigger service-provider requirements. Local providers must assess the tokens they offer and disclose relevant information about backing, redemption and holders' rights.

Copyright © Shufti. All Rights Reserved.

AML/CFT REQUIREMENTS FOR STABLECOIN BUSINESSES

- Providers handling stablecoins must meet applicable BCB AML/CFT requirements, including Circular 3,978, which cover customer and beneficial-owner identification, risk classification, politically exposed persons, transaction monitoring and suspicious-transaction reporting to COAF.
- For transfers involving self-hosted wallets, providers must identify the owner and keep documented processes to verify the assets' origin and destination. When dealing with virtual-asset providers abroad, they must check that the foreign entity is effectively supervised or document the risks of doing business with it.
- The Travel Rule applies in phases, with domestic information-transfer procedures due by 2 February 2027 and the international phase and full compliance due by 2 February 2028.
- Resolution 591 adds reporting of transfers to or from self-hosted wallets worth at least US$10,000, including qualifying stablecoin transfers, on top of suspicious-transaction reporting. Providers must report covered transfers contracted between 1 October and 31 December 2026 on the first business day of January 2027.
- From 6 November 2026, banks, payment institutions and other BCB-authorised institutions may not carry out, or help carry out, relevant virtual-asset operations with unauthorised providers, except under expressly permitted arrangements.

Copyright © Shufti. All Rights Reserved.

5. Stablecoin regulatory requirements by sector

Stablecoin regulatory requirements vary by sector because they depend on whether a business issues tokens, holds them for customers, facilitates exchange, processes payments or provides the rails on which other businesses build their products. Stablecoin issuers, banks, custodians and wallet providers, crypto exchanges, crypto card issuers, stablecoin payments platforms, and money service and remittance providers each face AML/CFT requirements alongside stablecoin rules on licences, permitted tokens and conduct. These requirements apply in certain jurisdictions rather than everywhere, so each point notes in general terms where it applies.

Stablecoin Issuers

Stablecoin rules and AML/CFT requirements for stablecoin issuers

Issuers create tokens when customers pay in money and destroy them when customers redeem their tokens for cash. They usually know the customers who mint directly with them, but redemption is harder because a token may have changed hands many times before someone asks to turn it back into cash. The currency a token is pegged to can also bring an issuer under another country's licensing regime, wherever the issuer is based.

AML/CFT REQUIREMENTS

Run a full AML/CFT programme

In certain jurisdictions, issuers count as financial institutions under AML law, so their programme must cover customer identification, due diligence, suspicious activity reporting and sanctions.

Check customers before issuing or redeeming

Issuers must complete due diligence before a business relationship starts, before occasional transactions at or above a set threshold, and whenever identity information is in doubt.

Copyright © Shufti. All Rights Reserved.

Monitor tokens after they leave the issuer

Some regimes call for monitoring across issuance, redemption and tokens in circulation, together with verification of each holder unless effective alternative controls satisfy the regulator.

Assess wallets and counterparties

Issuers must assess customer wallets, verify ownership or control where required, screen unhosted wallet addresses and check transfer counterparties.

Be able to block, freeze and reject

Issuers need the technical means, policies and procedures to stop unlawful transactions.

Screen, report and keep records

Issuers must keep sanctions controls in place, report suspicious transactions to the financial intelligence unit, and keep records.

Check whether AML law covers you

In the EU, e-money token issuers fall under AML law, whereas asset-referenced token issuers are not covered just because they issue ARTs.

STABLECOIN RULES

The peg currency can trigger a licence in another country

In certain jurisdictions, a stablecoin tied to the local currency needs a local licence wherever it is issued, or can only come from an issuer that the local central bank has licensed. Some markets also let foreign issuers serve local customers only if they come from a comparable regime and can comply with local orders.

Your customers may be in places where you cannot legally offer the token

In certain jurisdictions, regulators expect issuers to check location at onboarding and over time, including detecting customers who hide their location with VPNs. Issuers may also only issue some local-currency stablecoins to residents.

Copyright © Shufti. All Rights Reserved.

Banks

Stablecoin rules and AML/CFT requirements for banks

Banks deal with stablecoins in several roles, since they may issue them, hold issuers' reserves, run settlement accounts or receive the money when tokens are redeemed. Each role carries its own stablecoin rules, and whether a banking licence covers a given role differs from one market to the next.

AML/CFT REQUIREMENTS

Know the issuer behind the account

Industry guidance expects banks to understand an issuer's business and controls, the purpose of each account and the fund flows it should carry.

Meet crypto-service AML duties when offering custody or transfers

A bank that provides crypto services must meet the same AML/CFT and Travel Rule duties as other crypto service providers.

Apply stronger checks to higher-risk issuers

In higher-risk cases, banks may review the on-chain history of tokens before they are redeemed into fiat and check the source of large fiat deposits used to mint them.

Copyright © Shufti. All Rights Reserved.

STABLECOIN RULES

Issuing stablecoins under a banking licence works differently in each market

In certain jurisdictions, banks can only issue through an approved or separate subsidiary, while in others banks can become licensed issuers themselves or fall outside the stablecoin issuer regime altogether.

Some banks cannot deal with unauthorised crypto firms

In certain jurisdictions, the rules bar banks from dealing with crypto businesses that are not authorised or in the process of being authorised, which makes licence checks on crypto counterparties part of everyday banking compliance.

Offering stablecoin custody or conversion needs its own permission

In some markets, banks can notify their regulator instead of applying for a separate crypto licence, whereas in others they need specific central bank approval before converting stablecoins.

Banks can act as custodians of stablecoin reserves

Certain jurisdictions name banks as qualified custodians of stablecoin reserves.

Copyright © Shufti. All Rights Reserved.

Custodians and Wallet Providers

Stablecoin rules and AML/CFT requirements for custodians and wallet providers

Custodians and custodial wallet providers hold stablecoins or their reserves for others and move them on customers' instructions. Stablecoins bring rules for these firms that do not apply to other crypto assets: a stablecoin transfer can count as a payment, some markets limit which stablecoins can be held, and firms that hold issuers' reserves take on part of the issuer's rulebook.

AML/CFT REQUIREMENTS

Register for AML where required

In certain jurisdictions, firms that hold customers' tokens or private keys need AML registration, which a payments licence alone does not cover.

Verify and risk-assess customers

Custodians must verify customers and beneficial owners, assess risk, apply extra checks to PEPs and higher-risk customers, and monitor activity over time.

Apply the Travel Rule

Sender and recipient details must travel with transfers between providers, and in the EU this applies with no minimum amount.

Verify self-hosted wallets

In the EU, transfers above EUR 1,000 to or from a self-hosted wallet call for a check that the customer owns or controls it. In certain jurisdictions, providers must also identify the owner and assess the origin and destination of the funds.

Watch for multiple wallets

Some regulators treat one customer holding several wallets as a higher-risk feature.

Screen, report and keep records

Custodians must screen customers and wallet addresses against sanctions lists, report suspicious activity and keep records.

Copyright © Shufti. All Rights Reserved.

STABLECOIN RULES

Reserve custody for stablecoin issuers brings issuer-level standards

In certain jurisdictions, reserves must be kept separate from the custodian's own assets, protected from creditors and held by a qualified custodian that the issuer has checked.

Stablecoin holding and transfer services can need central bank permission

In certain jurisdictions, firms need a central bank licence or approval to hold and transfer stablecoins and may only transfer licensed or registered stablecoins, although supplying wallet software alone does not count as custody there.

A stablecoin transfer can count as a payment

In certain jurisdictions a stablecoin transfer counts as a payment, in which case the firm needs a payments licence on top of its crypto licence, or a licensed partner. Custodial wallets can also count as payment accounts.

Copyright © Shufti. All Rights Reserved.

Crypto Exchanges

Stablecoin rules and AML/CFT requirements for crypto exchanges

Most people buy and sell stablecoins on exchanges, and a growing number of markets now restrict which stablecoins exchanges can list and which customers can trade them. Decisions on listings and customer classification have therefore become compliance decisions in their own right.

AML/CFT REQUIREMENTS

Hold the right AML registration or authorisation

The registration varies by market and can mean CASP authorisation, AML registration, money services business registration or registration with FINTRAC.

Apply the Travel Rule and check counterparty providers

Exchanges must share required data on transfers and run due diligence on foreign crypto service providers where required.

Stop anonymous accounts

From 10 July 2027, EU rules ban anonymous crypto accounts and accounts that hide holders or transactions.

Verify and risk-assess customers

Exchanges must complete due diligence and beneficial ownership checks, apply enhanced checks to PEPs and keep monitoring customer activity.

Screen and report

Exchanges must screen customers, counterparties and wallet addresses, report suspicious activity and keep records.

Copyright © Shufti. All Rights Reserved.

STABLECOIN RULES

Some markets only allow stablecoins from authorised issuers

In certain jurisdictions, only stablecoins from authorised issuers may be offered or traded, and regulators there have told exchanges to stop trading non-compliant stablecoins after a short sell-only period.

Permitted-issuer rules turn listing into a compliance decision

Where these rules apply, exchanges need to review their stablecoin listings against the date from which only stablecoins from permitted issuers may be offered.

Some markets limit unlicensed stablecoins to professional investors

In those markets, exchanges must confirm which customers qualify as professional investors before offering them tokens from unlicensed issuers.

Some markets only allow fiat-backed stablecoins traded under regulator-set terms

In those markets, trading platforms may only let clients trade these stablecoins under the regulator's terms, which can include an undertaking the issuer has filed.

Stablecoin conversion can need central bank permission

In certain jurisdictions, exchanges need central bank approval before converting stablecoins, and stablecoins tied to foreign currencies may only be used to buy other crypto assets.

Some markets count stablecoin trades as foreign exchange

In those markets, exchanges must report each trade to the central bank, apply foreign exchange limits and give users clear information on holder rights and reserves.

Copyright © Shufti. All Rights Reserved.

Crypto Card Issuers

Stablecoin rules and AML/CFT requirements for crypto card issuers

Stablecoin-linked cards let people spend their token balance at ordinary shops because the programme behind each card usually converts the stablecoin into regular currency before or during the payment. Some markets treat that conversion, or the stablecoin payment itself, as a separately regulated activity.

AML/CFT REQUIREMENTS

Meet crypto-service AML duties where the programme exchanges or holds stablecoins

Due diligence, monitoring and reporting duties apply to the stablecoin side of the programme.

Monitor top-up, conversion and spend together

Card issuers must link unusual stablecoin funding and fast conversions to the cardholder's profile, and report suspicious activity.

Check the funding wallet

Card issuers must screen funding wallets for sanctions exposure and, in the EU, check ownership of self-hosted wallets for transfers above EUR 1,000.

Copyright © Shufti. All Rights Reserved.

STABLECOIN RULES

Stablecoin payments made through your card can count as payment services

Where they do, the programme needs a payments licence or a licensed partner, as described for custodians.

Some markets only let shops accept local-currency stablecoins

In those markets, the programme must convert stablecoins tied to foreign currencies before a card payment settles.

Card programmes that exchange or hold stablecoins can count as digital asset service providers

Where they do, permitted-issuer rules apply to the stablecoins behind these cards.

Card spending abroad settled in stablecoins can count as foreign exchange

In certain jurisdictions, these settlement transfers must be reported to the central bank like any other stablecoin foreign exchange operation.

A card licence may not cover the stablecoin behind the card

In certain jurisdictions, a retail payments or card licence does not cover converting or holding stablecoins, so that activity needs its own licence or regulatory approval.

Copyright © Shufti. All Rights Reserved.

Stablecoin Payments Platforms

Stablecoin rules and AML/CFT requirements for stablecoin payments platforms

Some businesses provide stablecoin rails to other financial firms instead of to the public. Through APIs, they offer virtual accounts, pay-ins and payouts, on- and off-ramps between fiat and stablecoins, instant stablecoin settlement, and custody and treasury tools. Wallets, exchanges and payment apps then build their own products on these services. These platforms often hold licences through separate entities in several markets, while the end users who move money through them are onboarded inside a client's app. The central compliance question is therefore who knows those end users and who answers for them.

AML/CFT REQUIREMENTS

Meet each local AML regime

Each licensed entity needs the registration and AML programme that its market prescribes.

Run KYB on client platforms

Platforms must verify each client business and its beneficial owners and confirm that the client holds the permissions its activity needs.

Own end-user due diligence unless reliance is lawful

A platform may rely on a regulated client's checks, but reliance does not cover outsourcing.

Apply the Travel Rule, including intermediary duties

Certain jurisdictions set specific duties for providers that pass transfers along the chain.

Screen, monitor and report

Platforms must screen parties and wallet addresses, monitor third-party pay-ins, report suspicious activity and keep records.

Copyright © Shufti. All Rights Reserved.

STABLECOIN RULES

Every on-ramp, off-ramp and settlement leg needs the right permission in each market

A fiat-to-stablecoin conversion carried out for clients can trigger the payment, conversion and foreign exchange rules described for custodians, exchanges and remittance providers, and the stablecoins you use for settlement must also be permitted in each client's market.

Copyright © Shufti. All Rights Reserved.

Money Service and Remittance Providers

Stablecoin rules and AML/CFT requirements for MSBs and remittance providers that settle in stablecoins

Scope: This section covers money services businesses and remittance providers that use stablecoins to settle payments, whether they settle with partners in stablecoins or send stablecoins directly to recipients.

Money services businesses and remittance providers can use stablecoins in two ways. In a settlement model, the sender pays in fiat currency, the provider uses stablecoins to settle with its partners and the recipient receives local currency, so neither customer needs to hold tokens. In a direct transfer model, the sender sends stablecoins to the recipient's wallet, where they can be held or converted into local currency.

AML/CFT REQUIREMENTS

Register and run an AML programme

In the US, this means FinCEN registration and a written programme with a compliance officer, staff training and independent testing, while Canada and the UK oblige providers to register with their AML supervisors.

Apply the Travel Rule on every qualifying transfer

For cross-border transfers between individuals above USD or EUR 1,000, the payment must carry names, addresses and dates of birth.

Verify senders and business customers

Providers must verify senders, and identify beneficial owners for business senders.

Screen every party

Providers must screen senders, recipients and wallet addresses against sanctions lists.

Copyright © Shufti. All Rights Reserved.

Assess token risks before offering token services

In the UAE, payment-token service providers must assess risks from anonymity, rapid cross-border transfers, peer-to-peer transfers and multiple wallets.

Report and keep records

Providers must file suspicious activity reports and keep the required records.

STABLECOIN RULES

The regulatory obligations of a stablecoin money service or remittance business depend on which entities collect funds, convert currencies, hold tokens, carry out transfers and deliver payouts, and on where those activities take place. Each provider therefore needs to assess the money transfer, cryptoasset and AML/CFT requirements that apply to its role in each corridor. A payments licence does not automatically cover additional cryptoasset activities, and in certain jurisdictions payment institutions that provide in-scope cryptoasset services must also register with their anti-money laundering supervisor.

Copyright © Shufti. All Rights Reserved.

Licensces a stablecoin money service or remittance business may need

European Union

A payment institution licence for money remittance, plus CASP authorisation for the stablecoin side, and a payments licence where euro stablecoin transfers count as payment services.

United Kingdom

Authorisation under the Payment Services Regulations 2017 for the fiat side, and FCA cryptoasset registration for the stablecoin side, moving to authorisation from October 2027.

United States

FinCEN money services business registration and state money transmitter licences, which also cover stablecoin transmission.

Singapore

A payment institution licence from MAS that covers both cross-border money transfer and digital payment token services.

Hong Kong

A money service operator licence from the Customs and Excise Department, alongside the stablecoin offering restrictions described in the Hong Kong section.

UAE

An exchange house licence from the CBUAE, plus a CBUAE non-objection registration before offering payment token services such as converting dirham stablecoins.

Canada

FINTRAC registration as a money services business, listing both remitting funds and dealing in virtual currencies among its registered activities.

Brazil

Authorisation to operate in the foreign exchange market, plus BCB authorisation as a virtual asset service provider.

Copyright © Shufti. All Rights Reserved.

6. Unique AML/CFT challenges for businesses operating in the stablecoin economy

Most AML/CFT obligations are common to the sectors that deal with stablecoins, because the same tokens pass between issuers, wallets, exchanges and payment providers. Whatever their role, these businesses generally need to verify and risk-assess their customers, exchange Travel Rule data with counterparties, screen the wallets involved in each transfer, monitor payments that move across fiat and on-chain rails, and decide when a partner's identity checks can be reused.

AML/CFT Challenges across all sectors



Copyright © Shufti. All Rights Reserved.

Customer due diligence

Challenges in verifying and assessing customers

REMOTE VERIFICATION OF INDIVIDUALS AND BUSINESSES

You have to identify and verify every customer, and for business customers that obligation extends to legal existence, ownership and control, beneficial owners and the authority of representatives. Remote onboarding makes each of these harder to prove, so document checks, face matching and liveness detection support remote KYC where appropriate.

RISK ASSESSMENT ACROSS PRODUCTS AND CORRIDORS

Customer risk depends on the purpose of the relationship, expected transaction values and volumes, funding sources and payment corridors. You need to assess customer, product, geographic and delivery-channel risks, including sanctions, politically exposed person and relevant adverse media findings. Higher-risk customers need enhanced due diligence, including source-of-funds or source-of-wealth checks and approvals appropriate to the risk.

ONGOING CUSTOMER INFORMATION UPDATES

You have to review customer information at appropriate intervals and whenever relevant circumstances change, and a new stablecoin service may call for an updated risk assessment and additional checks. Where the rules allow, existing verification can be reused instead of repeated (pp. 48–50).

Copyright © Shufti. All Rights Reserved.

Crypto Travel Rule

Challenges in exchanging sender and recipient information

COLLECTION AND EXCHANGE OF THE REQUIRED DATA	For qualifying stablecoin transfers, you have to collect the prescribed sender and recipient information, verify it where required, keep it and exchange it securely, usually off-chain to protect personal data. Data fields, thresholds and timing differ by jurisdiction and transfer type.
INTEROPERABILITY ACROSS TRAVEL RULE MESSAGING PROTOCOLS	Counterparties may use different Travel Rule messaging protocols, so data has to move securely across those systems, directly or through tested integrations. You need to map required information between message formats, tie each message to the correct transfer and track delivery failures, missing fields and counterparty responses. Any compatibility arrangement must preserve the information each jurisdiction prescribes.

Travel Rule exception handling

A sent Travel Rule message meets the obligation only when your workflow can also show that the required information is complete, attached to the correct transfer and available for review. Each missing field, failed delivery and counterparty that cannot receive data needs a named owner and a documented decision to retry, suspend, reject or return the transfer. Without that record, you cannot show a supervisor that you met your Travel Rule obligations for each transfer.

Copyright © Shufti. All Rights Reserved.

COUNTERPARTY VASP ASSESSMENT	You have to assess the receiving or sending virtual asset service provider for its legal identity, authorisation where required, jurisdiction, AML/CFT controls and ability to exchange Travel Rule data securely. A directory match or technical connection does not replace counterparty risk assessment.
PROOF OF WALLET OWNERSHIP OR CONTROL	A wallet address does not show who controls it. In the EU, a transfer above EUR 1,000 to or from a self-hosted wallet requires you to assess whether your customer owns or controls that wallet. Accepted methods include a message signed with the wallet's key and a small test transfer, and you should record the result and recheck it when ownership or risk changes.

Copyright © Shufti. All Rights Reserved.

Transaction monitoring

Challenges in monitoring stablecoin activity across payment rails

MONITORING RULES FOR EACH ACTIVITY

Your monitoring rules have to reflect the financial crime risks of the activities your business performs, such as remittances, merchant settlement, card funding and issuance or redemption. Rapid settlement becomes meaningful as a risk signal only when you assess it alongside customer history, expected activity, destinations and economic purpose.

Multi-rail transaction monitoring

A single stablecoin payment often has several legs, such as a fiat deposit, an on-chain transfer and a bank payout, and each leg can look ordinary when reviewed on its own. When you link every leg to the same customer, your teams can see the whole route the money took and identify unusual paths, shared beneficiaries and activity that does not fit the customer's profile. Where a partner supplies incomplete data for one of the legs, that gap should stay visible to investigators as a gap instead of being filled with assumptions.

SANCTIONS SCREENING OF WALLET ADDRESSES

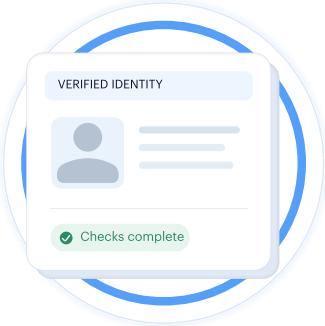
Sanctions screening has to cover wallet addresses as well as names. You have to screen the sending and receiving addresses before a transfer is released and again when lists change. Each confirmed match needs a documented decision to stop the transfer, freeze assets or file a report.

INTERPRETATION OF WALLET RISK SCORES AND CLUSTERS

Wallet risk scoring has to tell direct exposure from indirect exposure and account for data quality and network coverage. Wallet clustering can reveal connected flows or possible common control, although an exchange cluster may contain many customers' activity. Scores and clusters therefore support investigation without proving identity or wrongdoing.

Copyright © Shufti. All Rights Reserved.

Reusable KYC across stablecoin ecosystem partners



A single stablecoin payment often passes through several regulated businesses before it reaches the person being paid. The issuer mints the token, a wallet provider holds it, an infrastructure platform moves it, and a remittance, card or payment app serves the customer. Each of these businesses usually has its own customer due diligence duty, so the same person can be asked for the same identity document and selfie several times before one payment completes.

That repetition costs more than time. Customers can abandon onboarding when a second or third business asks for evidence they have already given, and every business that keeps its own copy adds another store of personal data to protect. Separate records also drift apart, so one business may hold an outdated address or a different risk rating for the same person, which weakens monitoring across the payment chain.

Stablecoin businesses also add products and corridors quickly. A remittance customer opens a wallet, a wallet user takes a card, and a holder who bought tokens elsewhere arrives at the issuer to redeem. Each of these moments decides whether the customer moves on with an identity that is already verified or starts onboarding again.

A new service should not always mean starting KYC again

A customer verified for a wallet may later want a card, a payment service or access through another app on the same platform, and a second round of document collection slows that customer down while adding little new information. Reusable KYC lets your business rely on identity evidence it already holds, as long as that evidence is still valid and the applicable rules permit its reuse. The new service still needs its own risk assessment, fresh sanctions and PEP screening where required, and any extra checks that the product's risk justifies.

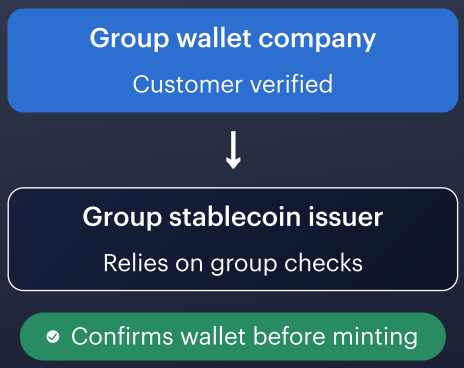
Copyright © Shufti. All Rights Reserved.

Reusable KYC across stablecoin groups, partners and products

Issuer and group wallet

One group-wide AML programme

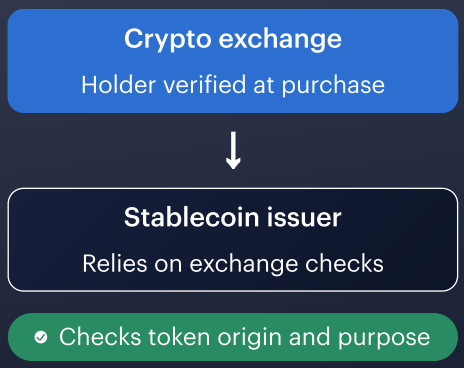
A customer verified by the group's wallet company can usually mint with the group's issuer without repeating onboarding, as one AML/CFT programme covers both. The issuer must still record the customer's wallet address and confirm the customer owns or controls it before minting.



Exchange and issuer

Holder verified elsewhere

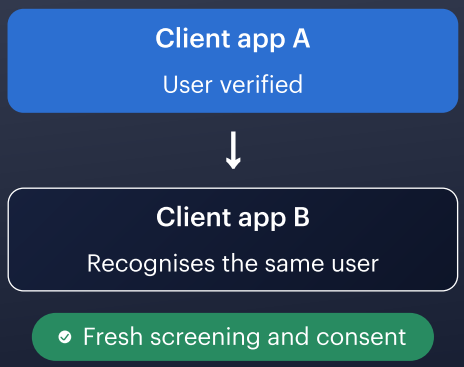
A holder who bought tokens on an exchange may come to the issuer only to redeem. Where the rules allow, the issuer can rely on the exchange's verification if the exchange is supervised for AML/CFT and shares the evidence straight away, but it still checks the tokens' origin and the reason for larger redemptions.



Infrastructure platform

Platform partner

A user already verified for one client's app can often be recognised when joining another app built on the same infrastructure platform, with fresh sanctions and PEP screening and data protection consent for the new app.

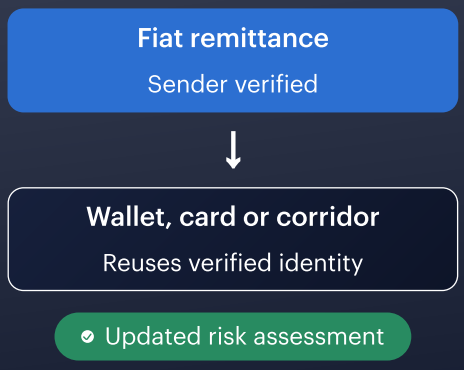


Copyright © Shufti. All Rights Reserved.

Remittance provider

Same business, new product

A sender first verified for fiat remittance may later open a stablecoin wallet, take a stablecoin-linked card or start using a new corridor. You can usually reuse the verified identity, then update the risk assessment for the new product and add stablecoin-specific checks.



Conditions for relying on another business's checks

The partner you rely on is regulated for AML/CFT. It is supervised or monitored for AML/CFT and has customer due diligence and record-keeping measures in place. [47]

Group reliance follows group standards. Within a financial group, your business can rely on customer due diligence and record-keeping standards that the group applies under a group-wide programme. [47]

Data sharing has a lawful basis. When you rely on another entity's checks, you must meet the applicable reliance and data protection requirements. [47]

Information is available straight away. Your business gets the necessary customer information immediately. It can also get copies of the identification evidence from the partner without delay on request. [47]

Reliance is not outsourcing. If a partner simply runs onboarding on your behalf, your business remains responsible for the checks. In certain jurisdictions, a licensed crypto provider also stays responsible for anything it outsources. [6, 47]

Evidence stays current. A new product, corridor or change in risk calls for updated information or additional checks before you reuse the evidence.

Copyright © Shufti. All Rights Reserved.

7. Shufti as compliance infrastructure for stablecoin businesses

Compliance obligations arise at each point in a stablecoin's life: when a token is minted, when it moves between wallets and providers, when it is converted to or from fiat, and at redemption or payout. Shufti provides identity and financial-crime compliance infrastructure for stablecoin issuers, banks, custodians and wallet providers, crypto exchanges, card issuers, payments and infrastructure platforms, and MSBs and remittance providers at each of those points. Verified identities and screening results stay linked to each customer record, and configured workflows send unresolved issues for review.

Copyright © Shufti. All Rights Reserved.

01

IDENTITY

Verify direct customers before minting and every holder before redemption

Issuers need to know who buys tokens directly and who cashes them out, including holders who first appear at redemption with no history on the platform. Document verification, facial matching and liveness establish identity at both points, with docless verification and address checks where supported. For direct issuance and redemption services, due diligence workflows support additional checks on the requesting customer and the transaction purpose, so those checks can finish before payout deadlines. Geolocation checks support configured access restrictions where a token cannot be offered in a customer's location.

02

KYB

Verify the platforms, distributors and partners between the issuer and the end user

Stablecoin arrangements depend on businesses in the middle: client fintechs building on infrastructure platforms, distributors selling an issuer's token, and conversion and payout partners in each corridor. KYB, UBO verification and business AML screening establish the entities and individuals behind each one, and due diligence workflows collect relationship purpose, expected activity and supporting evidence for higher-risk relationships.

03

REUSABLE KYC

Reuse verified identities across ecosystem partners without skipping product-level checks

Businesses often onboard the same person more than once, whether through an issuer and a wallet in the same group, several apps on one infrastructure platform, or an MSB adding a stablecoin wallet or card. Fast ID enables consent-based identity reuse within the configured business and partner ecosystem, and biometric re-verification connects returning customers to their verified records. Risk-based step-up checks request additional evidence where a new product needs it, which reduces repeated document collection while preserving product-specific due diligence.

Copyright © Shufti. All Rights Reserved.

04

WALLETS

Check wallet ownership and wallet risk before any stablecoin transfer

Stablecoins sent to a self-hosted wallet leave the regulated perimeter. Wallet screening checks addresses against sanctions lists and watchlists before a transaction is processed, with sanctioned-wallet lists refreshed every 15 minutes, and counterparty discovery helps identify a servicing VASP. For self-hosted wallets, cryptographic signatures and specified micro-transactions provide evidence of customer control. Each match links to the customer verified at onboarding, so reviewers assess wallet exposure and control alongside identity.

05

TRAVEL RULE

Exchange Travel Rule data on each qualifying stablecoin transfer between providers

Stablecoin transfers between providers carry the same Travel Rule duties as other virtual assets, and platforms acting for clients' end users also need to establish whose details travel with each transfer. Direct VASP messaging, TRP, CODE and Global Travel Rule (GTR) connectivity enable structured originator and beneficiary information exchange through one integration using IVMS101, while counterparty discovery and VASP risk assessment inform data-sharing decisions. Status tracking, examination-ready records and configured hold or escalation workflows let teams address incomplete exchanges and unavailable counterparties according to their compliance policies.

Copyright © Shufti. All Rights Reserved.

06

MONITORING

Monitor the fiat, on-chain and payout legs of a settlement as one customer journey

In settlement and remittance models, one payment can pass through a fiat deposit, a stablecoin transfer and a local-currency payout. Transaction Trust Monitoring assesses the linked records your business supplies against customer profiles, beneficiary history and corridor risk, with configurable scenarios for rapid conversion followed by withdrawal, split transfers, shared beneficiaries and departures from expected remittance volumes. Customer risk reassessment brings emerging activity into review priorities, and the Agentic Rule Builder lets teams draft scenarios and run historical tests. Where required information is missing, the record is flagged as Not Assessable.

07

OFF-RAMP

Protect the off-ramp where stablecoins return to fiat

Off-ramps are where account takeover and payout redirection turn into losses. Supported bank account ownership checks address beneficiary substitution when stablecoin proceeds return to fiat, and biometric re-verification strengthens withdrawal and account-change controls. Fraud network detection connects shared devices, network information and repeated biometric identities to reveal potential synthetic identity networks and mule-account relationships.

08

SCREENING

Keep screening holders and partners after onboarding

A customer or payout partner who was clear at onboarding can become a sanctions, PEP or adverse media match later. Ongoing AML screening identifies new matches involving enrolled customers and businesses, and linking the results to verified customer records gives analysts the identity context they need to decide whether further investigation, enhanced due diligence or other action is warranted.

Copyright © Shufti. All Rights Reserved.

Alert investigation with full payment context

An alert is harder to resolve when the customer's identity records, screening results and payment history sit in separate systems, because analysts then spend their time gathering evidence instead of assessing it. A single case that brings the relevant records together lets analysts judge the activity, document their reasoning and escalate with a clear record of what happened and why.

09

INVESTIGATIONS

Accelerate alert review with evidence ready for investigation

Case management brings customer history, screening results and linked transactions together so analysts can prioritise alerts. The AI Compliance Co-Pilot explains screening-hit classifications, while analysts and the MLRO keep final decision-making responsibility. Case management also preserves findings, escalation and closure rationale, and reporting workflows support SAR and STR preparation, with direct submission available through supported jurisdiction-specific connections.

10

WORKFLOWS

Adapt compliance workflows to the expansion of stablecoin services

Journey Builder lets teams configure separate verification steps, evidence requests and manual review for issuance, redemption, wallet and payout flows, and APIs and SDKs connect these workflows to existing systems. Deployment and data residency options support information-governance requirements, with availability confirmed for the selected services and configuration.

Copyright © Shufti. All Rights Reserved.

Many stablecoin businesses, particularly MSBs and remittance providers, may end up verifying the same customers again when they add a stablecoin balance, wallet or card. An exchange that launches a stablecoin-funded card, for example, can ask users it has already verified to upgrade their verification and upload fresh proof of address before the card is issued. Shufti Fast ID lets verified customers prove it's them with a single selfie, using patented reusable identity across brands and partners, and routes any unclear match to full KYC. Stablecoin businesses can then add products and corridors without putting customers through onboarding again, so Shufti works as a growth engine as well as a compliance engine for global leaders, including two of the top three global crypto exchanges.

To see how it fits your corridors, products and partners: **Request a Demo**



Copyright © Shufti. All Rights Reserved.

8. Stablecoin AML compliance solution checklist

Stablecoin issuers, banks, custodians and wallet providers, crypto exchanges, card issuers, payments platforms and remittance providers can use this checklist to assess whether an AML compliance solution covers what their business needs before they launch a service or expand into another corridor.

Tick each capability the solution offers, since any empty box is a gap it leaves open.

- ☐ **Your solution verifies customers before issuance and redemption.** Document verification, facial matching and liveness detection cover direct customers and holders who first appear at redemption, and geolocation checks support restrictions where a token cannot be offered.

- ☐ **Every business in your payment chain can be verified.** KYB, UBO verification and business AML screening cover client platforms, distributors and payout partners, and due diligence workflows record the purpose and expected activity of higher-risk relationships.

- ☐ **Sector-specific checks are covered for your business.** Tick the lines that apply.
  - ☐ Issuers can verify direct customers and every holder at redemption.
  - ☐ Banks can run enhanced due diligence on stablecoin issuers.
  - ☐ Custodians and wallet providers can verify self-hosted wallet ownership.
  - ☐ Exchanges can assess counterparty VASPs and screen wallet addresses.
  - ☐ Card issuers and payments platforms can run KYB on client businesses.
  - ☐ Remittance providers can screen senders, recipients and wallets per corridor.

Copyright © Shufti. All Rights Reserved.

- [ ] **Your solution reuses verified identities across partners and products.** Consent-based identity reuse lets a customer move between an issuer, a wallet and a payout partner without repeating onboarding, while step-up checks request more evidence where a new product needs it.

- [ ] **Wallets are screened before any funds move.** The solution checks sending and receiving addresses against sanctions lists and watchlists before a transaction is processed, and counterparty discovery helps identify the servicing VASP.

- [ ] **Control of self-hosted wallets can be proven.** The solution accepts a cryptographic signature or a specified micro-transaction as evidence of control and keeps that evidence linked to the customer verified at onboarding.

- [ ] **Travel Rule data moves across the protocols your counterparties use.** One integration exchanges originator and beneficiary data in the IVMS101 format, and status tracking shows when data is missing, delivery fails or a counterparty cannot be reached.

- [ ] **Every leg of a stablecoin payment is monitored as one journey.** The solution assesses the linked fiat, on-chain and payout records your business supplies, and its scenarios flag rapid conversion followed by withdrawal, split transfers and shared beneficiaries.

- [ ] **AML screening continues after onboarding.** Customers, businesses and beneficial owners stay under sanctions, PEP and adverse media screening for the life of the relationship, and every new match links back to the verified customer record.

Copyright © Shufti. All Rights Reserved.

- [ ] **Fraud and account takeover signals are detected.** Biometric re-verification protects withdrawals and account changes, bank account ownership checks address payout redirection, and fraud network detection connects shared devices and repeated biometric identities to reveal possible mule accounts.

- [ ] **Every alert arrives with full context in one case.** Case management brings identity records, screening results and linked transactions together, analysts keep the final decision on AI-assisted reviews, and reporting workflows support SAR and STR preparation.

- [ ] **Workflows adapt as you add products and corridors.** Teams can configure separate verification steps for issuance, redemption, wallet and payout flows, and APIs and SDKs connect those workflows to existing systems.

Copyright © Shufti. All Rights Reserved.

Shufti brings end-to-end compliance to crypto and stablecoin businesses

From onboarding through monitoring to assurance, Shufti's Glocal platform covers customer due diligence, AML screening and risk assessment, Travel Rule compliance and transaction monitoring for stablecoin businesses. It already serves crypto exchanges, stablecoin issuers, banks, and payment and remittance providers, including two of the top three global crypto exchanges.

Onboard with full customer due diligence

Verify individuals and businesses, identify beneficial owners and assess AML risk through sanctions, PEP and adverse media screening before the first mint, trade or transfer.

Monitor customer risk after onboarding

Ongoing AML screening and transaction monitoring show when a verified customer becomes a risk, with fraud and account takeover signals linked to each customer profile.

Assure transfers and payouts before funds move

Travel Rule compliance for qualifying transfers, wallet screening, bank account verification and biometric step-up checks confirm who is sending and receiving funds.

Grow your stablecoin operations with trust built in

Stablecoins are pegged to familiar currencies, so more people and businesses are starting to use digital assets through them. Shufti's compliance infrastructure, already trusted across these sectors, helps stablecoin businesses keep compliance seamless as that use grows.

Copyright © Shufti. All Rights Reserved.

9. References

Sources are grouped by area, with the guide pages where each area is covered.

Country	Regulations
Market data p. 03	Federal Reserve FEDS Notes on stablecoins in 2025 (2026)
Global standards pp. 09–12, 30	FATF Recommendation 16 revisions (2025) FATF report on stablecoins and unhosted wallets (2026) FATF seventh targeted update on virtual assets (2026) Wolfsberg guidance on banking stablecoin issuers (2025)
European Union pp. 13–14	MiCA, Regulation (EU) 2023/1114 Transfer of Funds Regulation (EU) 2023/1113 AMLR, Regulation (EU) 2024/1624 EBA Travel Rule guidelines, EBA/GL/2024/11 (2024) ESMA statement on non-MiCA-compliant stablecoins (2025)
United Kingdom pp. 15–16	FCA cryptoasset policy statements, incl. PS26/10 (2026) Money Laundering Regulations 2017 (SI 2017/692) Bank of England systemic stablecoin policy (2026)
United States pp. 17–18	GENIUS Act, Public Law 119-27 (2025) Treasury proposed AML and sanctions rules for issuers (2026) FinCEN guidance FIN-2019-G001 (2019)
Singapore pp. 19–20	MAS stablecoin regulatory framework (2023) MAS consultation on implementing legislation (2026)

Copyright © Shufti. All Rights Reserved.

Country	Regulations
Hong Kong pp. 21–22	Stablecoins Ordinance (2025) HKMA guideline on supervising licensed issuers (2025) HKMA AML/CFT guideline for licensed issuers (2025) HKMA grant of the first issuer licences (2026)
UAE pp. 23–24	CBUAE Payment Token Services Regulation (2024) VARA Virtual Asset Issuance Rulebook (2025)
Canada p. 25	Stablecoin Act, S.C. 2026, c. 3 (not yet in force)
Brazil pp. 26–27	BCB Resolutions 519, 520 and 521 (2025) BCB Circular 3,978 (2020) BCB Resolution 591 (2026)

Copyright © Shufti. All Rights Reserved.

Shufti



Shufti is based in the United Kingdom and operates offices worldwide.

United States
16200 SW Pacific Hwy, Suite H PMB 1053, Tigard, OR

Cyprus
Arch. Makarios III Avenue 229, Limassol

Dubai
Unit 507, Level 5, Gate District Precinct Building 03, DIFC, Dubai

Hong Kong
8 Queen's Road East, Wan Chai, Hong Kong

Pakistan
322-G3 Main Blvd, Johar Town, Lahore, Pakistan

Singapore
68 Circular Road #02-01, Singapore

United Kingdom
Office 408, Coppergate House, 10 Whites Row, London E1 7NF

Explore a Shufti solution
sales@shufti.com

Explore our products
shuftipro.com